PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-041934
(43)Date of publication of application : 13.02.1998

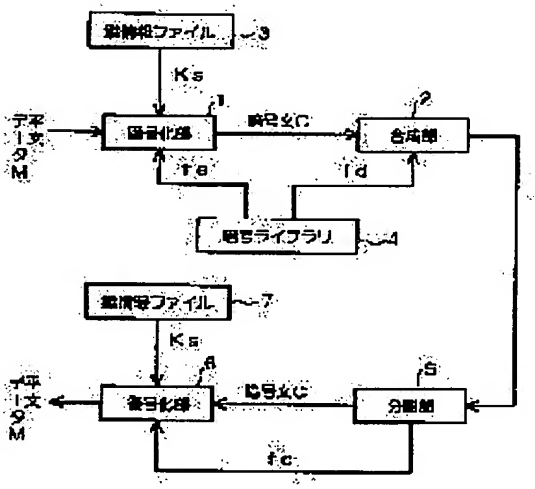
(51)Int.Cl. H04L 9/14
G06F 13/00
G09C 1/00
H04L 9/08
H04L 9/36

(21)Application number : 08-197854
(22)Date of filing : 26.07.1996

(71)Applicant : OKAMOTO EIJI
TOSHIBA CORP
(72)Inventor : OKAMOTO EIJI

(54) INFORMATION CIPHERING DECODING METHOD AND INFORMATION CIPHERING DECODER

(57)Abstract:
PROBLEM TO BE SOLVED: To easily attain ciphering decoding without giving load to a recipient of a cryptogram by using a decoding program and key information so as to decode the cryptogram into a plain text.
SOLUTION: A ciphering section 1 uses a ciphering program f2 of a ciphering algorithm E selected by a sender user of information from a program group stored in a ciphering library 4 and key information Ks stored in a key information file 3 to plain test data M. A synthesis section 2 synthesizes the cryptogram C which a decoding program fd of the ciphering algorithm E read from the ciphering liberary 4. The synthesized cryptogram C and the decoding program fd are sent to an information recipient. Then a separate section 5 separates received ciphering data into the cryptogram C and the decoding program fd. Moreover, a decoding section 6 decodes the cryptogram C separated by a separate section 5 by using the separated decoding program fd and the key information Ks stored in a key information file 7.



LEGAL STATUS

[Date of request for examination]	23.08.2000
[Date of sending the examiner's decision of rejection]	02.12.2003
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3537959

[Date of registration]	26.03.2004
[Number of appeal against examiner's decision of rejection]	2004-00264
[Date of requesting appeal against examiner's decision of rejection]	05.01.2004
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－41934

(43)公開日　平成10年(1998)２月13日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/14			Ｈ０４Ｌ	9/00	６４１
Ｇ０６Ｆ	13/00	３５１		Ｇ０６Ｆ	13/00	３５１Ｚ
Ｇ０９Ｃ	1/00	６６０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６６０Ｅ
Ｈ０４Ｌ	9/08			Ｈ０４Ｌ	9/00	６０１Ｚ
	9/36					６０１Ｅ

審査請求　未請求　請求項の数６　ＯＬ　（全７頁）　最終頁に続く

(21)出願番号　特願平8－197854

(22)出願日　平成８年(1996)７月26日

特許法第30条第１項適用申請有り　1996年１月29日～１月31日　電子情報通信学会情報セキュリティ研究専門委員会主催の「1996年暗号と情報セキュリティシンポジウム」において文書をもって発表

(71)出願人　596110280
岡本　栄司
石川県金沢市平和町２丁目28番60号　Ｂ39－12

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　岡本　栄司
石川県金沢市平和町２丁目28番60号　Ｂ39－12

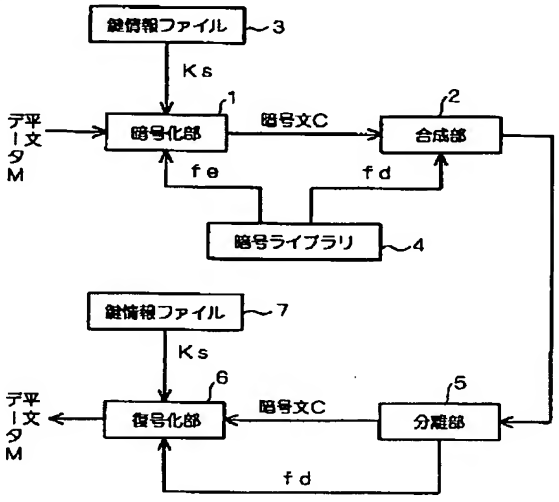
(74)代理人　弁理士　鈴江　武彦　（外６名）

(54)【発明の名称】　情報暗号化復号化方法および情報暗号化復号化装置

(57)【要約】

【課題】暗号文の受け手に負担をかけることなく、取り扱う情報の種類に応じた暗号化復号化が容易に行える情報暗号化復号化方法およびそれを用いた暗号化復号化装置を提供する。

【解決手段】情報の送り手により選択された複数の暗号化アルゴリズムのうちの１つと、前記鍵情報を用いて平文情報を暗号化する暗号化部１と、この暗号化部１で暗号化された暗号文と前記選択された暗号化アルゴリズムに対応する復号化プログラムを合成する合成部２と、この合成部２で合成された暗号文と復号化プログラムをネットワークあるいは記録媒体を介して受け取ると、これらを分離する分離部５と、この分離部５で分離された暗号文を前記分離部５で分離された復号化プログラムと前記鍵情報を用いて平文情報に復号する復号化部６とを具備する。



【特許請求の範囲】

【請求項１】　情報の送り手と受け手との間で予め定められた鍵情報をそれぞれ保持し、この鍵情報を用いて情報の送り手側で暗号化された情報を受け手側で復号する情報暗号化復号化方法において、

情報の送り手により選択された複数の暗号アルゴリズムのうちの１つと、前記鍵情報を用いて平文情報を暗号化して暗号文を生成し、この暗号文と前記選択された暗号アルゴリズムに対応する復号化プログラムを合成し、情報の受け手側で前記合成された暗号文と復号化プログラムをネットワークあるいは記録媒体を介して受け取ると、これらを分離し、前記暗号文を前記復号化プログラムと前記鍵情報を用いて平文情報に復号することを特徴とする情報暗号化復号化方法。

【請求項２】　情報の受け手側で、前記復号化プログラムはその復号化プログラムを実行するコンピュータの実行可能なコードに翻訳されて、その翻訳された復号化プログラムに従って前記暗号文の復号処理が実行されることを特徴とする請求項１記載の情報暗号化復号化方法。

【請求項３】　情報の受け手側で、前記復号化プログラムを実行するコンピュータのリソースへアクセスする前記復号化プログラム上の入出力命令を削除することを特徴とする請求項１記載の情報暗号化復号化方法。

【請求項４】　情報の送り手と受け手との間で予め定められた鍵情報をそれぞれ保持し、この鍵情報を用いて情報の送り手側で暗号化された情報を受け手側で復号する情報暗号化復号化装置において、

情報の送り手により選択された複数の暗号化アルゴリズムのうちの１つと、前記鍵情報を用いて平文情報を暗号化する暗号化手段と、

この暗号化手段で暗号化された暗号文と前記選択された暗号化アルゴリズムに対応する復号化プログラムを合成する合成手段と、

情報の受け手側で前記合成手段で合成された暗号文と復号化プログラムをネットワークあるいは記録媒体を介して受け取ると、これらを分離する分離手段と、

この分離手段で分離された暗号文を前記分離手段で分離された復号化プログラムと前記鍵情報を用いて平文情報に復号する復号化手段と、

を具備したことを特徴とする情報暗号化復号化装置。

【請求項５】　情報の受け手側で、前記復号化プログラムはその復号化プログラムを実行するコンピュータの実行可能なコードに翻訳されて、その翻訳された復号化プログラムに従って前記復号化手段で前記暗号文の復号処理が実行されることを特徴とする請求項４記載の情報暗号化復号化装置。

【請求項６】　情報の受け手側で、前記復号化プログラムを実行するコンピュータのリソースへアクセスする前記復号化プログラム上の入出力命令を削除することを特徴とする請求項４記載の情報暗号化復号化装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報の送り手と受け手との間で予め定められた鍵情報を保持し、この鍵情報を用いて情報の送り手側で暗号化された情報を受け手側で復号する情報暗号化復号化方法およびそれを用いた情報暗号化復号化装置に関する。

【０００２】

【従来の技術】コンピュータを中心とする各種情報機器の発達や情報関連技術の目覚しい発展、情報ネットワークの充実した基盤整備により、ネットワークを介した情報活動は日々活発になっている。また、それに伴い、我々の日常生活において扱われている情報そのものも、量的な増加は言うまでもなく、質的にも充実したものになりつつある。情報活動の主体であるコンピュータやネットワークのユーザも社会の各層に現れ、情報事業にたずさわる人口も増える一方である。

【０００３】このように情報活動がより身近なものになるに伴い、情報の盗聴、かいざん、なりすましなどの犯罪が行なわれる可能性が生じ、情報セキュリティ上の大きな脅威となっている。このような犯罪に対する防止及び予防の努力無くして安全な情報活動は確保できない。ネットワークにおいての情報セキュリティを確保する上での暗号システムの利用は一般的かつ強力な手段となる。現在、ＰＥＭ（Ｐｒｉｖａｃｙ　Ｅｎｈａｎｃｅｄ　Ｍａｉｌ）、ｓｅｃｕｒｅ　ＨＴＴＰ、ＰＧＰ（Ｐｒｅｔｔｙ　Ｇｏｏｄ　Ｐｒｉｖａｃｙ）などの暗号を利用した実用性に富んだシステムが注目を集めはじめている。

【０００４】しかし、これらの暗号系や秘密情報システムが世界のほとんど全てのネットワークを結ぶインターネットのユーザにとって自由に使える便利なものなわけではない。各ユーザが通信相手から送られてきた暗号文を復号し、平文を得るためには相手側が用いた暗号系を知っておかねばならないし、またそれに対応する復号装置を用意しなければならない。例えば、インターネット上のどんな相手とでも自由に暗号通信を行なおうとすると世界中で使われる暗号の全てに対応しなければならない。これは金と手間という二つのコストの増加を招きかねない。このことは暗号利用の促進を妨げる主な要因となっている。

【０００５】この問題を解決する方策として暗号系の標準化が考えられる。誰もが自由に使える標準的な暗号系がインターネット上に存在すれば良いわけであるが、標準的な暗号系は存在しないし、存在し得ない。なぜなら標準的な暗号の利用に対しては様々な障害や問題があるからである。主な障害要因としてあげられるのは、国家間の通商法やライセンス問題がある。

【０００６】このような法的な制約に加えて暗号に対するユーザの好みの問題がある。暗号の強度やスピード、

計算機の性能と利用技術の進展により暗号に対するユーザの信頼度も変化するので標準案の押しつけを嫌うユーザもいよう。

【０００７】

【発明が解決しようとする課題】現在のメールシステムは国や地域を超えてネットワークがつながっていれば世界中のどこにもメールを送ることが可能になっている。このメールシステムのような共通ツールが暗号システムに存在すれば、誰もが快く利用できるわけであるが、上記したような様々な問題により標準的な暗号系の出現は困難である。

【０００８】標準的な暗号系がない故に暗号システムの利用者、特に暗号文の受信者は、通信相手が用いるであろうほとんど全ての暗号系に対する復号装置を用意しなければならない。これは金と手間というコストの増加を招くので暗号の利用そのものを妨げる要因でもある。上記の権利問題に制限されず、しかも個人の好みまで満足できる方式があれば暗号の利用はよりオープンにかつ自由になるであろう。

【０００９】また、画像、音声、データ、プログラムなど、容量も形式もまちまちな情報を取り扱うこれからのマルチメディア通信を考えると、これら各々に対して、暗号化復号化を行うための装置を送受信側に用意するのは容易ではない。特に、情報消費の意味で受信側が一般ユーザとなるケースが多い状況では、受信側に負担をかけない情報保護機構が求められることになる。

【００１０】そこで、本発明は、上記問題点に鑑みてなされたものであり、暗号文の受け手に負担をかけることなく、取り扱う情報の種類に応じた暗号化復号化が容易に行える情報暗号化復号化方法およびそれを用いた暗号化復号化装置を提供することを目的とする。

【００１１】

【課題を解決するための手段】本発明の情報暗号化復号化方法は、情報の送り手と受け手との間で予め定められた鍵情報をそれぞれ保持し、この鍵情報を用いて情報の送り手側で暗号化された情報を受け手側で復号する情報暗号化復号化方法において、情報の送り手により選択された複数の暗号アルゴリズムのうちの１つと、前記鍵情報を用いて平文情報を暗号化して暗号文を生成し、この暗号文と前記選択された暗号アルゴリズムに対応する復号化プログラムを合成し、情報の受け手側で前記合成された暗号文と復号化プログラムをネットワークあるいは記録媒体を介して受け取ると、これらを分離し、前記暗号文を前記復号化プログラムと前記鍵情報を用いて平文情報に復号することにより、暗号文の受け手に負担をかけることなく、取り扱う情報の種類に応じた暗号化復号化が容易に行える。

【００１２】また、本発明の情報暗号化復号化装置は、情報の送り手と受け手との間で予め定められた鍵情報をそれぞれ保持し、この鍵情報を用いて情報の送り手側で暗号化された情報を受け手側で復号する情報暗号化復号化装置において、情報の送り手により選択された複数の暗号化アルゴリズムのうちの１つと、前記鍵情報を用いて平文情報を暗号化する暗号化手段と、この暗号化手段で暗号化された暗号文と前記選択された暗号化アルゴリズムに対応する復号化プログラムを合成する合成手段と、情報の受け手側で前記合成手段で合成された暗号文と復号化プログラムをネットワークあるいは記録媒体を介して受け取ると、これらを分離する分離手段と、この分離手段で分離された暗号文を前記分離手段で分離された復号化プログラムと前記鍵情報を用いて平文情報に復号する復号化手段と、を具備することにより、暗号文の受け手に負担をかけることなく、取り扱う情報の種類に応じた暗号化復号化が容易に行える。

【００１３】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して説明する。一般に、暗号系には、対称暗号系と非対称暗号系がある。暗号化鍵と復号化鍵のいずれか一方から他方を容易に求められる暗号系を対称暗号系（ｓｙｍｍｅｔｒｉｃ　ｃｒｙｐｔｏｓｙｓｔｅｍ）、容易に求められない暗号系を非対称暗号系（ａｓｙｍｍｅｔｒｉｃ　ｃｒｙｐｔｏｓｙｓｔｅｍ）と呼ぶ。最近、鍵を送る必要のない公開鍵暗号方式が注目を集めているが、本発明では特定の暗号系に依存しない方式を提案し、実装の対象としている。また、暗号通信に先立って鍵の生成のため、暗号系を持っていなければならない公開鍵暗号方式は対象外とする。

【００１４】本発明の実施形態に係る情報暗号化復号化装置は、情報の送り手から受け手へ、暗号文とそれを復号するアルゴリズムを同時に送ることにより、特定の暗号系に依存することなく、また、復号のための受信側の負担の軽減が図れるものであり、ここでは、特に、ネットワークを介する暗号通信（例えばメールシステム）の場合を例にとり説明する。

【００１５】図１は、本発明の情報暗号化復号化方法を用いた情報暗号化復号化装置の機能構成を概略的に示したブロック図である。情報の送り手側には、少なくとも暗号化部１、合成部２、鍵情報ファイル３、暗号ライブラリ４を具備し、情報の受け手側には、少なくとも分離部５、復号化部６、鍵情報ファイル７を具備している。

【００１６】暗号ライブラリ４には、例えば、ＦＥＡＬ（Ｆａｓｔ　ｄａｔａ　Ｅｎｃｉｐｈｅｒｍｅｎｔ　Ａｌｇｏｒｉｔｈｍ）、ＮＦＳＲ（Ｎｏｎ－ｌｉｎｅａｒ　Ｆｅｅｄｂａｃｋ　Ｓｈｉｆｔ　Ｒｅｇｉｓｔｅｒｓ）等の暗号アルゴリズムを記述したプログラム（平文を暗号化して暗号文を生成する暗号化プログラムとそれに対応して、暗号文を平文に復号化する復号化プログラム）群が記憶されている。

【００１７】鍵情報ファイル３、７には、情報の送り手と受け手との間で予め定められた鍵情報がそれぞれ記憶

されている。暗号化部１は、暗号ライブラリ４に記憶されているプログラム群から情報の送り手側のユーザにより選択された暗号アルゴリズムＥの暗号化プログラムｆｅと、鍵情報ファイル３に記憶されている鍵情報Ｋｓを用いて平文データＭを暗号化するものである。

【００１８】合成部２は、暗号化部１で暗号化されて出力された暗号文Ｃを暗号ライブラリ４から読み出された暗号アルゴリズムＥの復号化プログラムｆｄと合成するようになっている。

【００１９】合成部２で合成された暗号文Ｃと復号化プログラムｆｄ（以下、この合成されたものを暗号データと呼ぶ）は、所定のネットワークを介して情報の受け手側に送信される。

【００２０】分離部５は、ネットワークを介して受信した暗号データを暗号文Ｃと復号化プログラムｆｄに分離するものである。復号化部６は、分離部５で分離された暗号文Ｃを、同じく分離部５で分離された復号化プログラムｆｄと鍵情報ファイル７に記憶された鍵情報Ｋｓを用いて復号化するようになっている。

【００２１】さて、ここで、本発明の情報暗号化復号化方法をソフトウエアにて実現し、それをパーソナルコンピュータ等に実装することにより情報暗号化復号化装置を構成する場合、そのソフトウエアの構成上の特徴について説明する。

【００２２】１）　プログラムの記述

例えば、インターネットのように、ほとんど全てのユーザに対応できるネットワークを介して暗号文と復号化プログラムを同時に転送する場合、そのネットワークには、どのような端末がつながっているかわからないので、少なくとも復号化プログラムは暗号データの受け手側の端末のＯＳやマイクロプロセッサに依存しない（マシン依存性のない）記述形式のものが望ましい。

【００２３】そのために、本発明では、暗号データの受け手に仮想マシンを持たせ、それが解析・処理するマシン語でプログラムを記述するものとする。このマシン語で記述されたプログラムは暗号データの受け手側の端末（コンピュータ）に設けられた仮想マシンが理解できるもので、実際のコンピュータ上で実行するには、このマシン語を解釈し、コンピュータが理解できるコードにさらに翻訳し、これをコンピュータに渡して実行させる機能（インタプリタ）が必要である。少なくともこのような機能を具備したソフトウエアを、ここでは、仮想マシンと呼ぶ。

【００２４】２）　既存のシステム（メールシステム等）に対する安全対策

インターネット等のネットワークを介して他の端末から送られてきた復号化プログラムを実行する際、そのプログラムによって、受け手側の端末のシステムが破壊されないことが要求される。例えば、復号化プログラム中の、どのメモリの記憶領域に格納されているデータやプログラムを削除しろとか、どこのデータやプログラムが格納されているメモリの記憶領域に重ね書きしろ、といった形の命令は、そのプログラムを実行することにより、システム設定ファイルを書き換えられたり、ファイルを削除されたりすることがある。

【００２５】その対策として、本発明では、復号化プログラムを実際に実行する際に、例えば、インタプリタでの実行時に、そのプログラム中のコードを解析して、メモリ、ハードディスク、プリンタ等のコンピュータのリソースを操作するコード、すなわち、既存のシステムを破壊する可能性のあるコードをチェックし、削除することで、受け手側のユーザのシステムを保護するようにする。

【００２６】このように、インタプリタの実行時にプログラム上に不当なリソースへのアクセスを行うような不当なコードがないかどうかをチェックおよび必要に応じて削除することは、ウイルス侵入の防護壁ともなるであろう。

【００２７】３）　鍵情報の管理

本発明の目的とするところは、特定の暗号処理系に依存することのない情報暗号化復号化が行えることである。そのために、暗号方式は鍵の生成に特定の暗号系を必要としない対称暗号系を、鍵の管理はローカルに行う必要がある。

【００２８】そこで、本発明では、ファイル保護機能を持たない環境下でも鍵情報ファイル３を保護するためにパスワードを用いることとする。図２は、本発明の情報暗号化復号化方法を実現するソフトウエアの構成例を示したものであり、仮想マシン１０、ユーザインタフェイス１１、鍵情報ファイル１２、暗号ライブラリ１３から構成される。図２の鍵情報ファイル１２は、図１の鍵情報ファイル３、７に相当し、図２の暗号ライブラリ１３は、図１の暗号ライブラリ４に相当する。

【００２９】仮想マシン１０は、前述したようにインタプリタの機能を具備したもので、例えば、プログラミング言語Ｓｃｈｅｍｅを用いることができる。プログラミング言語　Ｓｃｈｅｍｅは、Ｃｏｍｍｏｎ　Ｌｉｓｐとともにプログラミング言語Ｌｉｓｐ（Ｌｉｓｔ　Ｐｒｏｃｅｓｓｏｒ）の標準言語である。Ｌｉｓｐは名のとおり、リスト処理を得意とする言語である。リストはそれ自身は単なるモノ（データ）の並びにすぎないが、使い次第非常に複雑な情報を容易にしかも効率よく表現できるという特性をもっている。この特性のためプログラミング言語Ｌｉｓｐは、記号処理分野、特に、エキスパートシステムをはじめとする人工知能システム、数式処理システム、定理証明システム、機械翻訳システムなどの開発に用いられてきた。しかし、その利用範囲は、記号処理だけに限られたわけでなく、数値計算、グラフィックス、テキスト・エディタをはじめとする文書処理、システム・プログラミングなどでも使われている（湯浅太

一；”Ｓｃｈｅｍｅ入門”岩波書店、１９９１）。

【００３０】仮想マシンとして言語Ｓｃｈｅｍｅ（ＳＣＭ　ｖｅｒｓｉｏｎ　４ｅｌ）を採用できるのは、次のような特徴を持っているからである。

１．特定のマシンやＯＳに依存しない処理系でほとんど全ての計算機上で動くように設計されている。

【００３１】２．アルゴリズムの記述がシンプルにできる。

３．データの型や扱える数の大きさに制限がほとんどないので、かなり大きい整数が簡単に扱えるので暗号アルゴリズムの記述に向いている。

【００３２】４．暗号文をもＳｃｈｅｍｅのプログラムの一部として記述できるのでメモリ等のリソースに対する入出力命令に頼らなくてすみ、送信文の構成がしやすい。

ＳＣＭは、ＭＩＴのＡｕｂｒｅｙ　Ｊａｆｆｅｒが創った言語である。ＳＣＭは、Ａｌｇｏｒｉｔｈｍｉｃ　Ｌａｎｇｕａｇｅ　Ｓｃｈｅｍｅに関するレポート（Ｒｅｖｉｓｅｄ　４　Ｒｅｐｏｒｔ）とＩＥＥＥ　ｐ．１１７８の仕様にしたがって設計された（Ａｕｂｒｅｙ　Ｊａｆｆｅｒ；Ｏｎｌｉｎｅ　ＭＡＮＵＡＬ　ｆｏｒ　ＳＣＭ　ｖｅｒｓｉｏｎ　４ｅｌ、ＭＩＴ．１９９４）。小型のＬｉｓｐでありながら処理スピートや機能は優れている。

【００３３】ユーザインタフェイス１１は、ユーザに使いやすい環境を提供するものであり、暗号系とは独立に存在するもので、多くのユーティリティ機能を備えたインターフェースである。ユーザはこれを持たなくても暗号ライブラリとエディターなどがあれば、暗号化、送信、復号化を行うことができるが、ユーザインタフェイス１１を使用することによりこのような手間を省くことができる。

【００３４】次に、ユーザインタフェイス１１の具体的な機能を以下に説明する。

１．鍵情報の管理：鍵情報の新規登録、変更、削除などを行なう。例えば、通信相手のメールアドレスとともに鍵情報は、鍵情報ファイル１２というファイルに暗号化されて格納される。この際、暗号鍵となるのがパスワードである。

【００３５】２．パスワードの管理：ＰＣ（Ｐｅｒｓｏｎａｌ　Ｃｏｍｐｕｔｅｒ）のようにファイルの保護機能を持たない環境下でも、鍵情報ファイルを保護するためにパスワードを用いている。

【００３６】３．図１の暗号化部１、合成部２、分離部５、復号化部６の各機能を仮想マシン１０との協調動作により実現する。

４．メールの伝送代行や受信メールの解析機能：受信した通信文には、暗号文やアルゴリズムだけでなくメールヘッダなどがついている。メールヘッダには、受信した時間や通信相手のＩＤなどの情報が書かれてある。ユーザインタフェイス１１は、通信相手のメールＩＤを拾い、鍵情報ファイル１２からその通信相手との間で予め定められてた鍵情報を捜して復号作業を行なう。

【００３７】５．有害なコマンドコードのチェック機能（既存のシステムに対する安全対策）：送られた復号化プログラムを実行することにより受信者側のコンピュータシステムが被害を被ることがあり得る。例えば、システム設定ファイルを書き換えられたり、必要なファイルが削除されたりすることが挙げられる。ユーザインタフェイス１１は、送られてきたプログラムからこのような被害を与え得るコマンドコードをチェックし、削除することでユーザのシステムを保護する。また、ユーザインタフェイス１１の出力はファイルに書き込まれず、画面のみに表示されるようになっている。

【００３８】暗号ライブラリ１３は、図１で説明したように、暗号アルゴリズムを記述したプログラム（平文を暗号化して暗号文を生成する暗号化プログラムとそれに対応して、暗号文を平文に復号化する復号化プログラム）群が格納されているもので、ある。仮想マシン１０に、例えば、Ｓｃｈｅｍｅ言語　が用いられている場合、暗号ライブラリ１３のプログラム群もＳｃｈｅｍｅ言語で書かれたものである。

【００３９】若干のルールを守れば誰でも新しい暗号アルゴリズムを追加できるようになっている。ユーザは好きな暗号アルゴリズムを例えば、Ｓｃｈｅｍｅで書き、このライブラリに加えることができる。

【００４０】この暗号（復号）化プログラムを書く上で、例えば、以下のような規則を設けてもよい。

１．復号化プログラムは、”（ｄｅｆｉｎｅ”文で始まらなければならない。ユーザインタフェイス１１、仮想マシン１０は、これを見つけたらプログラムの始まりと認識する。

【００４１】２．復号化プログラムの最後に、ユーザインタフェイス１１、仮想マシン１０に知らせるシンボル“ｅｎｄ＜ｓｍａｉｌ＞”を書かなければならない。メールシステムによって付けられるメールの終端の印など余計な情報を削除するためである。

【００４２】３．暗号化プログラムが生成する暗号文や復号化プログラムには一定数（実装においては１００に固定）の文字毎に改行マークを出力するようにしなければならない。メールシステムのラインバッファの大きさに制限があるため、メールシステムを経由して送られる情報が途中で切られる恐れがあるからである。

【００４３】４．暗号ライブラリ１３の中の暗号化プログラムと復号化プログラムとを別々に書き、暗号化には暗号化プログラムを使い、復号化には復号化プログラムを使うようにする。インターフェースとライブラリとを完全に分離するためである。

【００４４】図２に示すような構成のソフトウエアは、情報の送り手側および受け手側のコンピュータに実装さ

れる必要がある。次に、図１、図２に示した情報暗号化復号化装置の処理動作を図３および図４に示すフローチャートを参照して説明する。

【００４５】情報の送り手側のユーザは、自端末（コンピュータ）で、例えば、電子メール文を作成してそれを暗号化して相手端末に転送する際に、まず、ユーザインタフェイス１１を呼び出す。そして、ユーザインタフェイス１１を介してその端末に具備されている所定のディスプレイ装置に操作案内等が表示されると、それをもとに、暗号ライブラリ１３に格納されている複数の暗号アルゴリズムの中から、処理対象の電子メール文（平文データＭ）を暗号化するための暗号アルゴリズムＥを１つ選択する（図３のステップＳ１）。さらに、その電子メール文の送り先（通信相手のＩＤ、アドレス等）を指定する。

【００４６】ユーザインタフェイス１１では、例えば、通信相手のＩＤを基に、鍵情報ファイル１２からその通信相手との間で予め定められてた鍵情報Ｋｓを検索し（ステップＳ２）、また、暗号ライブラリ１３からユーザにより選択された暗号アルゴリズムＥの暗号化プログラムｆｅを読み出して、平文データＭに対し暗号処理を行い、暗号文Ｃを生成する（ステップＳ３）。

【００４７】ユーザインタフェイス１１では、さらに、暗号ライブラリ１３から、ユーザにより選択された暗号アルゴリズムＥの復号化プログラムｆｄを読み出して、それと暗号文Ｃを合成し、メールヘッダを付加して所定のネットワークを介して相手端末に転送する（ステップＳ４）。

【００４８】情報の受け手側の端末が所定のネットワークを介して暗号文Ｃと復号化プログラムｆｄが合成された通信文（暗号データ）を受信すると（図４のステップＳ１０）、自動的にユーザインタフェイス１１が呼び出され（ステップＳ１１）、ユーザインタフェイス１１は、暗号データを暗号文Ｃと復号化プログラムｆｄに分離する（ステップＳ１２）。

【００４９】復号化プログラムｆｄは、仮想マシン１０に具備されたインタプリタで受け手側の端末が実行可能なコード（実行可能プログラム）に翻訳される（ステップＳ１３）。その際、前述したように、プログラム上の有害なコマンドコード等のチェックおよび削除行う（ステップＳ１４）。

【００５０】一方、ユーザインタフェイス１１は、通信文に付加れていたメールヘッダに記述された送り元のメールＩＤを基に、鍵情報ファイル１２からその通信相手との間で予め定められてた鍵情報Ｋｓを読み出しておく（ステップＳ１５）。

【００５１】この鍵情報Ｋｓと仮想マシン１０で実行可能プログラムに翻訳された復号化プログラムｆｄを用いて暗号文Ｃを平文データＭに復号する（ステップＳ１６）。以上説明したように、上記実施形態によれば、暗号文を送る側のユーザは、自分が用いることのできる、あるいは用いたい暗号系を使って、暗号文を生成し、暗号文とともに復号化プログラムも同時に送り、受け手側の端末では、送られた復号化プログラムと予め通信相手との間で定められた鍵情報を使い、暗号文から平文を得ることにより、受け手側は、相手が用いた暗号系の種類について何の情報も必要としないし、権利問題などについて制限されることはないので全く負担はなくなる。また、受け取った復号化プログラム上にあるメモリ等のリソースへのアクセスコマンドコードをチェックし、必要に応じて削除することにより既存のメールシステムをそのまま利用できるのみならず、既存のシステムに何の影響も及ぼすことがない。従って、暗号文の受け手に負担をかけることなく、取り扱う情報の種類に応じた暗号化復号化が容易に行える。

【００５２】予め送り手側と受け手側が鍵情報を示し合わせておき、他の人に漏らさなければ安全に通信できる。また、受け手側は、予め復号装置を用意しておく必要がなく単に鍵情報を入力すれば元の情報が得られるので、非常に負担が軽くなる。さらに、情報の送り手側は好きな暗号を選択あるいは作成できるという利点もある。

【００５３】なお、上記実施形態では、既存のメールシステムを用いた電子メール文の暗号通信を例にとり説明したが、この場合に限らず、本発明の情報暗号化復号化方法は、情報の送り手側で、暗号文と復号化プログラムを合成したものをフロッピーディスク、ＣＤＲＯＭ等の記録媒体に保存し、その記録媒体を介して情報の受け渡しを行う場合にも適用できる。

【００５４】

【発明の効果】以上説明したように、本発明によれば、暗号文の受け手に負担をかけることなく、取り扱う情報の種類に応じた暗号化復号化が容易に行える情報暗号化復号化方法およびそれを用いた暗号化復号化システムを提供できる。

【図面の簡単な説明】

【図１】本発明の実施形態に係る情報暗号化復号化装置の機能構成を概略的に示したブロック図。

【図２】本発明の実施形態に係る情報暗号化復号化方法を実現するソフトウエアの構成例を示した図。

【図３】情報暗号化復号化装置の処理動作を説明するためのフローチャートで、情報の送り手側の処理動作を示したものである。

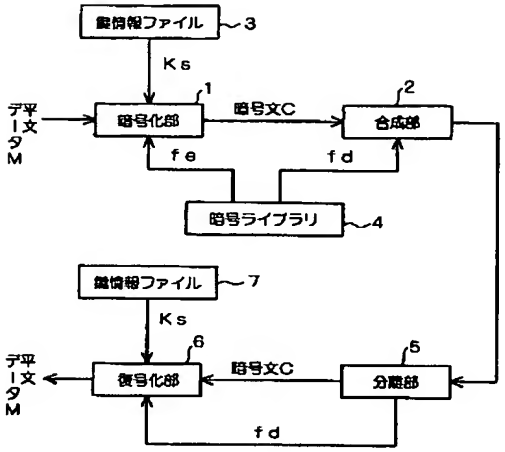
【図４】情報暗号化復号化装置の処理動作を説明するためのフローチャートで、情報の受け手側の処理動作を示したものである。

【符号の説明】

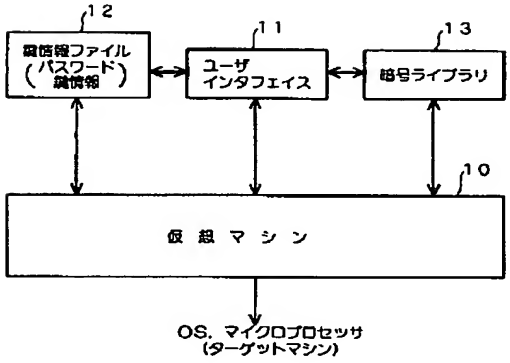
１…暗号化部、２…合成部、３…鍵情報ファイル、４…暗号ライブラリ、５…分離部、６…復号化部、７…鍵情報ファイル、１０…仮想マシン、１１…ユーザインタフ

エイス、１２…鍵情報ファイル、１３…暗号ライブラリ、Ｍ…平文データ、Ｃ…暗号文、Ｋｓ…鍵情報。

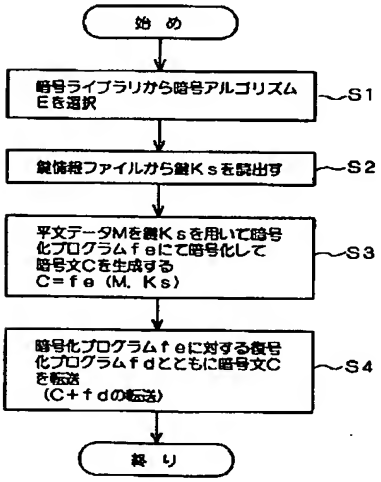
【図１】



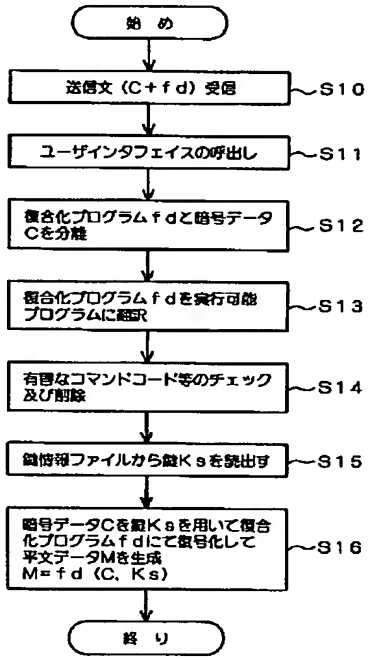
【図２】



【図３】



【図４】



フロントページの続き

(51)Int.Cl.[6]	識別記号	庁内整理番号	FI		技術表示箇所
			H04L 9/00	685	